(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 June 2005 (16.06.2005)

PCT

(10) International Publication Number
WO 2005/055512 A2

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US2004/040279

(22) International Filing Date: 1 December 2004 (01.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/526,301 1 December 2003 (01.12.2003) US
Not furnished 30 November 2004 (30.11.2004) US

(71) Applicant *(for all designated States except US)*: THE REGENTS OF THE UNIVERSITY OF CALIFORNIA [US/US]; 1111 Franklin Street, 12th Floor, Oakland, California 94607 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BRESSON, Emmanuel [FR/FR]; CELAR, F-35174 Bruz (FR). CHEVASSUT, Olivier [FR/US]; 5719 Keith Avenue, Oakland, California 94618 (US). POINTCHEVAL, David [FR/FR]; 29, rue Victor Basch, F-94320 Thiais (FR).

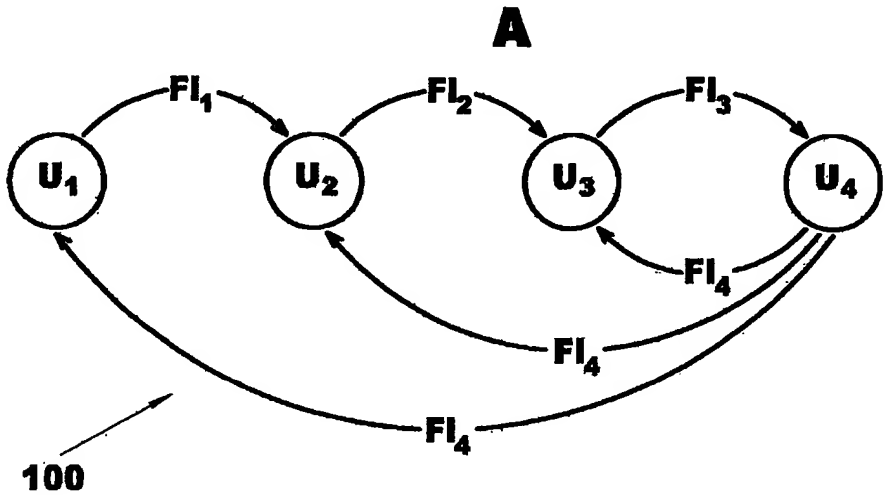
(74) Agents: MILNER, Joseph et al.; Lawrence Berkeley National Laboratory, One Cyclotron Road, Mail Stop 90B-0104, Berkeley, California 94720-8127 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: CRYPTOGRAPHY FOR SECURE DYNAMIC GROUP COMMUNICATIONS



(57) Abstract: Cryptographic dynamic group communications are disclosed, where: 1) a first player U_1 initiates an upflow to the next player, the upflow based on a random value χ_1, a random value v_1, and "g", a generator of a finite cyclic group where a computational solution to a Diffie-Hellman problem is hard; 2) each player after the first U_p sends an upflow Fl_p, comprising information based on a random values χ_p, v_p, and the previous upflow Fl_{p-1}; and 3) the last player U_n sends a downflow Fl_n to all other players in the dynamic group, where the downflow Fl_n comprises information based on a random values χ_n, v_n, and the previous upflow Fl_{n-1}. Players may be added to or removed from the dynamic group by adjusting the downflow to the remaining players. The dynamic groups may be refreshed and/or merged by adjusting the downflow.

WO 2005/055512 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PATENT APPLICATION

CRYPTOGRAPHY FOR SECURE DYNAMIC GROUP COMMUNICATIONS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims benefit of priority to United States provisional patent application 60/526,301, "Cryptography for secure dynamic group communications: method, apparatus, and signal", filed 12/1/2003 and United States patent application __/___,___ entitled "Cryptography for secure dynamic group communications", filed 11/30/2004.

STATEMENT REGARDING FEDERAL FUNDING

[0002] This invention was made with U.S. Government support under Contract Number DE-AC03-76SF00098 between the U.S. Department of Energy and The Regents of the University of California for the management and operation of the Lawrence Berkeley National Laboratory. The U.S. Government has certain rights in this invention.

REFERENCE TO A COMPUTER PROGRAM

[0003] Not Applicable.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0004] The present invention relates to provably secure communications, and more particularly relates to secure communications among dynamic groups.

2. Description of the relevant art

[0005] US patent 5,241,599 discloses a method which permits computer users to authenticate themselves to a computer system without requiring that the computer system keep confidential the password files used to authenticate the respective user's

identities. The 5,440,635 invention is useful in that it prevents a compromised password file from being leveraged by crafty hackers to penetrate the computer system.

[0006] US patent 5,440,635 discloses a cryptographic communication system, which employs a combination of public and private key cryptography, allowing two players, who share only a relatively insecure password, to bootstrap a computationally secure cryptographic system over an insecure network. The 5,440,635 system is secure against active and passive attacks, and has the property that the password is protected against offline "dictionary" attacks.

[0007] US patent 6,226,383 discloses a cryptographic method, where two players use a small shared secret (S) to mutually authenticate one another other over an insecure network. The 6,226,383 methods are secure against off-line dictionary attack and incorporate an otherwise unauthenticated public key distribution system.

[0008] One major difficulty with the preceding patents, and other representative technology, is that none of them scale very well to groups of more than two players intercommunicating with a secure encrypted method which is provably secure.

[0009] Publication "Group Diffie-Hellman Key Exchange Secure Against Dictionary Attacks" by Bresson, Chevassut, and Pointcheval, discloses a cryptographic communication system, which may be secure against "dictionary" attacks.

[0010] Publication "Mutual Authentication and Group Key Exchange for Low-Power Mobile Devices" by Bresson, Chevassut, Essiari, and Pointcheval, discloses a cryptographic communication system for low computational power devices.

[0011] The mathematic field of algebraic groups contains several terms in colloquial use that are used in this patent application. Such terms are "Finite Group", "Cyclic Group", "Group Order", "Group", "Abelian Group", and "Identity Element". These terms are used to describe the mathematics behind the concept of a finite group or a finite cyclic group with prime generator "g".

BRIEF SUMMARY OF THE INVENTION

[0012] This invention provides for a method for generating a cryptographic key by a player in a dynamic group, the method comprising: receiving, by a player U_p in a dynamic group with a first player U_1 and a last player U_n, where $p>1$, a previous upflow $\mathbf{Fl}_{p-1}$ from a previous player U_{p-1} in the dynamic group; player U_p selecting a random value x_p , and a random value v_p ; and player U_p sending an outflow $\mathbf{Fl}_p$, comprising information based on the random value x_p , the random value v_p , and the previous upflow $\mathbf{Fl}_{p-1}$. The first player U_1 may be a process on a computer that seeks to initiate a dynamic group, that in turn communicates with U_2 who may be either a user on the same computer, or another process on the same computer. In this instance, the last player, U_n would be a third or greater player. Dynamic groups of players may variously have size ranges from 1-2, 1-3, 3-20, 1-100, 1-1000 or more. Specifically, dynamic groups may initiate with 3 or more players, with subsequent departure of players, resulting in a dynamic group of 2 players. Similarly, dynamic groups may initiate with a single player, increasing to a dynamic group of 2 players may subsequently increase or decrease in number.

[0013] The method for generating a cryptographic key by a player in the dynamic group of paragraph [0012] , may further comprise: for a first player U_1 in the dynamic group: player U_p selecting a random value x_1 , and a random value v_1 ; setting an initial upflow $\mathbf{Fl}_1$ comprising information based on the random value x_1 , the random value v_1 , and "g", a generator of a finite cyclic group where a computational solution to a Diffie-Hellman problem is hard.

[0014] In the method for generating a cryptographic key by a player in the dynamic group of paragraph [0013] , the sending step may further comprise: when player U_p is not the last player in the dynamic group, then: player U_p sending an upflow $\mathbf{Fl}_p$ to a subsequent player U_{p+1} in the dynamic group, the upflow $\mathbf{Fl}_p$ comprising the outflow $\mathbf{Fl}_p$; when player U_p is the last player in the dynamic group, then: player U_p sending a downflow $\mathbf{Fl}_n$ to all other players in the dynamic group, the downflow $\mathbf{Fl}_n$ comprising the outflow $\mathbf{Fl}_p$.

[0015] In the method for generating a cryptographic key by a player in the dynamic group above, one or more players may be deleted by steps comprising: forming a set of L players, U_L , leaving the dynamic group; forming a set of R players,

U_R, remaining in the dynamic group; choosing a controller U_C from the remaining set of R players U_R; inputting, by controller U_C, the downflow $\mathbf{Fl}_n$, where the downflow $\mathbf{Fl}_n$ has one entry associated with each player in the dynamic group; and sending a controller U_C downflow signal $\mathbf{Fl}'_C$, comprising: controller U_C sending the controller downflow $\mathbf{Fl}'_C$ based upon a random value x_C, a random value v_C, and the downflow signal $\mathbf{Fl}_n$, where each entry associated with the set of L players U_L leaving in the downflow signal $\mathbf{Fl}_n$ has been deleted.

[0016] In the method for generating a cryptographic key by a player in the dynamic group above, one ore more players may be added by steps comprising: forming a set of J players to form a larger dynamic gropu $U_1, \ldots U_n, U_{n+1}, \ldots, U_{n+k}, \ldots, U_{n+J}$, where $1 \leq k \leq J$; sending an upflow $\mathbf{Fl}_{n+k}$ from each player U_{n+k}, to player U_{n+k+1}, where $1 \leq k < J-1$, said upflow $\mathbf{Fl}_{n+k}$ based upon a random value x_{n+k}, a random value v_{n+k}, and the upflow $\mathbf{Fl}_{n+k-1}$ received from player U_{n+k-1}; and sending a downflow $\mathbf{Fl}_{n+J}$ by player U_{n+J}, based upon a random value x_{n+J}, a random value v_{n+J}, and the upflow $\mathbf{Fl}_{n+J-1}$.

[0017] In the method for generating a cryptographic key by a player in the dynamic group above, all players may be refreshed with a new cryptographic key by steps comprising: choosing a refresher U_r from the dynamic group $U_1, \ldots U_n$; inputting, by refresher U_r, the downflow $\mathbf{Fl}_n$, where the downflow $\mathbf{Fl}_n$ has one entry associated with each player in the dynamic group; and sending, by refresher U_r, a refresher U_r downflow $\mathbf{Fl}'_r$ based upon a random value x_r, a random value v_r, and the downflow signal $\mathbf{Fl}_n$.

[0018] In the methods above for generating a cryptographic key wherein said upflows may be encrypted with a first encryption method. Alternatively, the downflows may be encrypted with a second encryption method, or still, both upflows and downflows may be encrypted with a single encryption method. Outflows may also be encrypted by either the first, second, or an entirely different encryption method. Any of these encryption methods may be based on symmetric-key, elliptic curve symmetric-key, or public key encryption methods.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0019] The invention will be more fully understood by reference to the following drawings, which are for illustrative purposes only:

[0020] Fig. 1A is a schematic of the flows involved in a secure dynamic group of four players.

[0021] Fig. 1B is a schematic of the flows involved in a secure dynamic group of four players where player two has been deleted, and player four has been designated as the group controller.

[0022] Fig. 1C is a schematic of the flows involved in a secure dynamic group of four players where player two has been deleted, and player three has been designated as the group controller.

[0023] Fig. 2A is a schematic of the flows involved in a secure dynamic group of two players.

[0024] Fig. 2B is a schematic of the flows involved in a secure dynamic group of two players adding another two players.

[0025] Fig. 3 is a schematic of three secure dynamic groups in communication through players who are members of two of the groups.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Definitions

[0026] "Computer" means any device capable of performing the steps, methods, or producing signals as described herein, including but not limited to: a microprocessor, a microcontroller, a digital state machine, a field programmable gate array (FGPA), a digital signal processor, a collocated integrated memory system with microprocessor and analog or digital output device, a distributed memory system with microprocessor and analog or digital output device connected by digital or analog signal protocols.

[0027] "Computer readable media" means any source of organized information that may be processed by a computer to perform the steps described herein to result

in, store, perform logical operations upon, or transmit, a flow or a signal flow, including but not limited to: random access memory (RAM), read only memory (ROM), a magnetically readable storage system; optically readable storage media such as punch cards or printed matter readable by direct methods or methods of optical character recognition; other optical storage media such as a compact disc (CD), a digital versatile disc (DVD), a rewritable CD and/or DVD; electrically readable media such as programmable read only memories (PROMs), electrically erasable programmable read only memories (EEPROMs), field programmable gate arrays (FGPAs), flash random access memory (flash RAM); and information transmitted by electromagnetic or optical methods including, but not limited to, wireless transmission, copper wires, and optical fibers.

[0028] "Player" means any person using, or any computer process residing, on a client or server computer. Multiple players may reside on the same or different computers, and multiple instances of a control process or person may be so designated.

[0029] "Dynamic Group" means a collection of players communicating together, where one or more players may be added or deleted singly or in subgroups.

[0030] "Finite Group" means a group of finite order n defined by an element g, the group generator, and its n powers, up to $g^n = I$, where I is the identity element. Further details regarding group theory, finite, and finite cyclic groups, may be obtained in mathematical treatises on algebraic group theory.

Secure Group Encryption Setup

[0031] One aspect of this invention is a secure group setup protocol. In this aspect, an initial static group of players desire to exchange a cryptographic key using a group password *pw*, which is known to all players. Initially, a base "g" is chosen, where "g" is a generator of a finite cyclic group. Generator "g" is additionally a high order prime number chosen so as to make a solution of the Diffie-Hellman problem computationally hard.

[0032] A plurality of players $U_1, \ldots U_j, \ldots, U_n$, where $1 \leq j \leq n$ are defined to be players U_j of the n players comprising a secure group.

[0033] The secure group is set up in the following manner. A first player, U_1, uses a generator "g", selects a random value x_1, and a random value v_1. Player U_1 then sends an initial upflow signal $\mathbf{Fl}_1$ from player U_1 to player U_2, where the initial upflow signal $\mathbf{Fl}_1$ is based upon generator "g", the random value χ_1, and the random value v_1.

[0034] Similarly, for player U_2 through player U_{n-1}, each player U_j selects a random value χ_j, and a random value v_j. Player U_j then sends an upflow signal $\mathbf{Fl}_j$ from player U_j to player U_{j+1}. The upflow signal $\mathbf{Fl}_j$ includes information based upon the preceding player U_{j-1} upflow $\mathbf{Fl}_{j-1}$, the random value χ_j, and the random value v_j.

[0035] In a functionally equivalent manner, the preceding method describing the steps from player U_2 to player U_{n-1} may instead be taken as though from player U_1 through player U_{n-1} by the simple expedient of setting $\mathbf{Fl}_0$ to be the generator "g".

[0036] The final player, U_n, takes as an input the preceding player U_{n-1} upflow $\mathbf{Fl}_{n-1}$. Player U_n selects a random value χ_n, and a random value v_n. Player U_n then broadcasts a downflow signal $\mathbf{Fl}_n$ to the remaining players (also known as a multicast when substantially simultaneously broadcast to multiple players) in the plurality of players $U_1 \ldots U_{n-1}$. Downflow signal $\mathbf{Fl}_n$ includes information based upon the preceding player U_{n-1} upflow $\mathbf{Fl}_{n-1}$, the random value χ_n, and the random value v_n.

[0037] Once a player U_j has received the downflow signal $\mathbf{Fl}_n$, player U_j may calculate a cryptographic key for use in secure group communications based on the downflow signal $\mathbf{Fl}_n$, and its previously selected random value χ_j. At this point, player U_j may be thought of as having connected to the group.

[0038] In the description above, the upflows may be unencrypted, encrypted by a first encryption method, or indeed encrypted with a different encryption method between each successive player U_j to U_{j+1}. Similarly, the downflow may be encrypted with a second encryption method, the same first encryption method, or indeed no encryption whatsoever. At this time, the literature has shown proof of security where the upflows and downflow are protected by encryption methods. Examples of such encryption methods include, but are not limited to, the Diffie-Hellman key exchange method, elliptic curve-based Diffie-Hellman methods, public key encryption methods, etc.

Detailed Description of the Flows

[0039] Each flow sent from a player U_j is dependent on the incoming upflow U_{j-1}, and the two selected random values χ_j and v_j, with the understanding that Fl_0 is comprised of generator "g". Table 1 below demonstrates this previous player dependency for a simple example case of four players:

Table 1. Flows Associated With Four Players

Fl_0	g			
Fl_1	g^{v_1}	$g^{v_1 x_1}$		
Fl_2	$g^{v_1 v_2 x_2}$	$g^{v_1 v_2 x_1}$	$g^{v_1 v_2 x_1 x_2}$	
Fl_3	$g^{v_1 v_2 v_3 x_2 x_3}$	$g^{v_1 v_2 v_3 x_1 x_3}$	$g^{v_1 v_2 v_3 x_1 x_2}$	$g^{v_1 v_2 v_3 x_1 x_2 x_3}$
Fl_4	$g^{v_1 v_2 v_3 v_4 x_2 x_3 x_4}$	$g^{v_1 v_2 v_3 v_4 x_1 x_3 x_4}$	$g^{v_1 v_2 v_3 v_4 x_1 x_2 x_4}$	$g^{v_1 v_2 v_3 v_4 x_1 x_2 x_3}$
Term →	β_1	β_2	β_3	β_4

[0040] In Table 1 above, each term $\beta_1 \ldots \beta_4$ in each flow is a single-valued number evaluated by exponentiation of the generator "g" as indicated. Thus, Fl_3 can be seen to have four numbers. Each of the players $U_1 \ldots U_4$ may have the downflow Fl_4 sent to them in either a sequential or a multicast manner. Additionally, U_4 may also send the downflow Fl_4 to itself should that be advantageous.

[0041] Each of the players U_k at this point has available to it a term β_k in the downflow Fl_4 corresponding to player U_k, as well as its previously selected random value χ_k. A cryptographic key is generated by raising the term β_k corresponding to the player U_k in the downflow to the power χ_k.

[0042] As an example, still referring to Table 1 above, player U_1 has term β_1 in the downflow of $g^{v_1 v_2 v_3 v_4 x_2 x_3 x_4}$, notably without any χ_1 exponent. By raising β_1 to the χ_1 power, we obtain $\left(g^{v_1 v_2 v_3 v_4 x_2 x_3 x_4}\right)^{x_1}$, or more simply $g^{v_1 v_2 v_3 v_4 x_1 x_2 x_3 x_4}$, which is the cryptographic key for player U_1, and indeed, all of the other players $U_1 \ldots U_4$. Thus,

all players have the same cryptographic key, and may commence communications with the key using Data Encryption Standard (DES), Advanced Encryption Standard (AES), or other encryption method, based upon the cryptographic key. From the cryptographic key $g^{\nu_1\nu_2\nu_3\nu_4 x_1 x_2 x_3 x_4}$, a session key may be calculated.

[0043] Refer now to Figure 1A, which depicts the setup phase of the four players described previously in Table 1. Flow $\mathbf{Fl}_1$ originates with player U_1, and is propagated to player U_2. Similarly, player U_2 originates flow $\mathbf{Fl}_2$, which is propagated to player U_3, and U_3 originates flow $\mathbf{Fl}_3$, which is propagated to player U_4. U_4 is shown as either sequentially broadcasting the downflow $\mathbf{Fl}_4$ to players U_1, U_2, and U_3, or simultaneously multicasting the downflow $\mathbf{Fl}_4$ to players U_1, U_2, and U_3. When a player U_1, U_2, and U_3 receives the downflow $\mathbf{Fl}_4$ and has generated the cryptographic key for a secure group session, the secure group 100 is established, and is ready for intragroup secure communication.

Secure Group Deletion

[0044] As may also be observed from Table 1 above, no term in any of the flows $\mathbf{Fl}_1$ ... $\mathbf{Fl}_4$ is repeated, and each flow term β_k is distinct. This distinctiveness property increases the difficulty of "cracking" the secure group cryptographic key, as none of the data values are repeated. Note that for each of the players U_k where $k = 1...4$, none of the flow terms β_k vertically above player U_k contains any exponentiation using χ_k.

[0045] To delete a player U_j, the downflow (in this example $\mathbf{Fl}_4$) has the term β_j associated with the player U_j deleted. Additionally, one of the remaining players is designated as the group controller (denoted "gc" in subscripts). After the downflow has been redacted of the one or more players leaving the group, the group controller selects a new random value χ_{gc}, and a new random value ν_{gc}. Using the previously obtained random values χ_{gc} and ν_{gc} used to enter the secure group, the resulting redacted flow is adjusted by raising each remaining term β_j having exponent χ_{gc}, to the power $\frac{\chi'_{gc}}{\chi_{gc}} \frac{\nu'_{gc}}{\nu_{gc}}$. For each remaining term β_j not having an exponent term containing χ_{gc}, (i.e. where $j = gc$) the redacted flow term β_j is adjusted by being exponentiated to the power $\frac{\nu'_{gc}}{\nu_{gc}}$.

[0046] The group controller may be chosen arbitrarily, but may also be chosen for reasons of security, computational power, logistical reasons, or convenience.

[0047] Refer now to Table 2 below, where, as an example, player U_2 is leaving the original four player secure group session described above. The group controller, here taken as player U_4, selects new values χ'_4, and a new random value r'_4, and adjusts the redacted downflow Fl'_{4-2}. The Fl'_{4-2} notation reflects a new flow including information based on the original downflow Fl_4 with player U_2 having been removed.

Table 2. Four Original Players With Player Two Redacted

Fl_4 original	$g^{r_1r_2r_3r_4x_2x_3x_4}$	$g^{r_1r_2r_3r_4x_1x_3x_4}$	$g^{r_1r_2r_3r_4x_1x_2x_4}$	$g^{r_1r_2r_3r_4x_1x_2x_3}$
Fl_{4-2} redacted	$g^{r_1r_2r_3r_4x_2x_3x_4}$	$g^{r_1r_2r_3r_4x_1x_3x_4}$	$g^{r_1r_2r_3r_4x_1x_2x_4}$	$g^{r_1r_2r_3r_4x_1x_2x_3}$
Fl'_{4-2} redacted	$g^{r_1r_2r_3r'_4x_2x_3x'_4}$	$g^{r_1r_2r_3r'_4x_1x_3x_4}$	$g^{r_1r_2r_3r'_4x_1x_2x'_4}$	$g^{r_1r_2r_3r'_4x_1x_2x_3}$
Player →	U_1	U_2	U_3	U_4
Term →	β_1	β_2	β_3	β_4

[0048] The deleted secure dynamic group that results is shown below, and denoted with primes to indicate the change in the group state. This updated state is then broadcast to the remaining group players.

[0049] Note that in this example, redaction is conceptually indicated by crossing out the cell containing the corresponding term in Table 2. While actual deletion of the corresponding term in the redacted outflow Fl_{4-2} is one option for forming the redacted outflow Fl'_{4-2}, it may also be formed by simply outputting the other terms of the redacted outflow, and skipping over the term(s) corresponding to the player(s) being deleted. Restating this, in the skipping method, the term β_2 is never actually deleted, merely skipped over and not included in the downflow Fl'_{4-2}. In either event, Table 3 shows the resulting downflow Fl'_{4-2} terms comprising the actual flow.

Table 3. Multicast Resulting From Four Original Players With Player Two Redacted

Fl'_{4-2}	$g^{r_1r_2r_3r'_4x_2x_3x'_4}$	$g^{r_1r_2r_3r'_4x_1x_2x'_4}$	$g^{r_1r_2r_3r'_4x_1x_2x_3}$
Player' →	U'_1	U'_3	U'_4

[0050] Refer now to Figure 1B, which graphically indicates the removal of player U_2 previously described in Tables 2 and 3. In this case, player U_4 has been designated as the group controller, and been renamed as U_{gc}. The adjusted downflow, having player U_2 redacted, is denoted Fl'_{gc}, which is either sequentially or simultaneously broadcast to players U_1 and U_3. Once a player has received the adjusted downflow Fl'_{gc} and has calculated a new cryptographic key, intragroup communications may be either commenced or resumed in the redacted group 130.

[0051] Refer now to Figure 1C, which graphically indicates the removal of player U_2. In this case, player U_3 has been designated as the group controller, and been renamed as U_{gc}. The adjusted downflow, having player U_2 redacted, is again denoted Fl'_{gc}, which is either sequentially or simultaneously broadcast to players U_1 and U_4. Once a player has received the adjusted downflow Fl'_{gc} and has calculated a new cryptographic key, intragroup communications may be either commenced or resumed in the redacted group 170. The resulting group 170 is functionally equivalent to group 130 described above in Figure 1B, with the exception that the cryptographic key and downflow Fl'_{gc} terms will be entirely different.

[0052] In the example above, player U_2 has been shown as actually removed. In practice, the player(s) being removed need just be skipped over in the multicast updated flow. After a player determines that it is no longer a member of the secure group, it would preferably delete all references and data relating to the group. As implied, this process may be used for several players leaving a dynamic secure group simultaneously, with the proviso that at least one player remain in the dynamic secure group. Additionally, the removal steps may be combined with the joining operations described below.

Secure Group Refresh

[0053] It may readily be seen that in the trivial case where no party is leaving, the previous steps of selecting a group controller, picking new random values for the group controller, and updating the downflow to the other group members has the effect of refreshing all downflow terms, and thereby refreshing the cryptographic key. Insofar as a hacker trying to break the cryptographic key, this has the effect of starting the attack all over, with no history whatsoever. This refresh technique may be useful if it appears that the secure group is under attack, or if there have been a number of unsuccessful joining events (joining is described below).

Secure Group Joining

[0054] Generally speaking, a set of J new players may join an existing plurality of players $U_1 \ldots U_n$ to form an expanded plurality of players $U_1 \ldots U_n, U_{n+1} \ldots U_{n+k} \ldots U_{n+J}$, where $1 \leq k \leq J$. In this process, one or more players are added to an ongoing group of players $U_1 \ldots U_n$, so that both the existing and new players may communicate among the expanded secure group.

[0055] A method used to join new players $U_{n+k}, \ldots, U_{n+J}$, where $1 \leq k \leq J$ to an existing group $U_1 \ldots U_n$ of n players comprises choosing one of the existing group players to act as a group controller U_{gc}. The group controller has available to it the initial group downflow $\mathbf{Fl}_n$, as do all players of the initial group. The group controller U_{gc} selects a new value χ'_{gc}, a new random value v'_{gc}, and adjusts the initial downflow with the new χ'_{gc} and v'_{gc}, values. As the initial downflow $\mathbf{Fl}_n$ is adjusted, the cryptographic key term missing from the initial flow is added. The resulting adjusted flow $\mathbf{Fl}'_{gc}$ is then sent to the first new player U_{n+1}, in the expanded secure group.

[0056] For players U_{n+1} through player U_{n+J-1}, each player U_{n+k} selects a random value χ_{n+k}, and a random value v_{n+k}. Player U_{n+k} then sends an upflow signal $\mathbf{Fl}'_{n+k}$ from player U_{n+k} to player U_{n+k+1}. The upflow signal $\mathbf{Fl}'_{n+k}$ comprises information based upon the preceding player U_{n+k-1} upflow $\mathbf{Fl}'_{n+k-1}$, the random value χ_{n+k}, and the random value v_{n+k}.

[0057] The final player in the expanded group, U_{n+J}, takes as an input the preceding player U_{n+J-1} upflow $\mathbf{FI'}_{n+J-1}$. Player U_{n+J} selects a random value χ_{n+J}, and a random value v_{n+J}. Player U_{n+J} then broadcasts a downflow signal $\mathbf{FI'}_{n+J}$ to the remaining players (also known as a multicast) in the expanded plurality of players U_1, ... U_n, U_{n+1}, ..., U_{n+k}, ..., U_{n+J}, where $1 \leq k \leq J-1$. Downflow signal $\mathbf{FI'}_{n+J}$ comprises information based upon the preceding player U_{n+J-1} upflow $\mathbf{FI'}_{n+J-1}$, the random value χ_{n+J}, and the random value v_{n+J}. Broadcast from the final player U_{n+J} in the expanded group to itself if not necessary, but may also be done.

[0058] Once a player U_j has received the downflow signal $\mathbf{FI'}_{n+J}$, player U_j may calculate a cryptographic key for use in secure group communications based on the downflow signal $\mathbf{FI'}_{n+J}$, and its previously selected random value χ_j.

[0059] In the description above, as with the initial setup of the secure group, the upflows may be unencrypted, encrypted by a first encryption method, or indeed encrypted with a different encryption method between each successive player U_j to U_{j+1}.

[0060] Similarly, the downflow may be encrypted with a second encryption method, the same first encryption method, or indeed no encryption whatsoever. At this time, the literature has shown proof of security where the upflows and downflow are protected by symmetric key encryption methods. Examples of such symmetric key encryption methods include the Diffie-Hellman method, elliptic curve-based Diffie-Hellman methods, etc.

[0061] The method described above for forming an expanded group is likely easier to understand with an example. Refer now to Figures 2A, 2B, and Table 4, which illustrate the steps and flows involved in expanding a secure group of two players to a secure group of four players.

[0062] In Figure 2A, we see an initial secure group 200 comprised of two players U_1 and U_2. In this very simple example $\mathbf{FI}_1$ player U_1 transmits an upflow $\mathbf{FI}_1$ to player U_2. Player U_2 responds by in turn transmitting a downflow $\mathbf{FI}_2$ to player U_1. After both players have calculated the cryptographic key, secure communications may commence between them.

[0063] Table 4 details the two flows between players U_1 and U_2 that comprise this initial secure group 200 with Fl_1 and Fl_2. In this example, the two flows comprise two exponentiated terms. As usual, the zeroth flow Fl_0 is set to comprise g.

[0064] Figure 2B indicates the addition of two more players to the secure group, forming a secure group 250 comprising four players: U_1, U_2, U'_3 and U'_4. All new components in this Figure are reflected with primed notation. Thus, we see that players U'_3, U'_4, and flows Fl'_2, Fl'_3, and Fl'_3 are new. In this example, player U_2 is designated as the group controller.

[0065] Player U_2 forms the adjusted flow, denoted as "Fl'_2 Adjusted" comprising information based on a new random value χ'_2, a new random value v'_2, and the previous downflow Fl_2, denoted in Table 4 as "Fl_2 Initial". Player U_2, acting as the group controller, then sends an upflow signal Fl'_3 to player U'_3. Player U'_3 then forms a new upflow, Fl'_3, comprising information based on a random value χ'_3, a random value v'_3, and the previous upflow "Fl'_2 Adjusted". Player U'_3 then sends upflow signal Fl'_3 to player U'_4.

[0066] Player U'_4 then forms a new downflow, Fl'_4, comprising information based on a random value χ'_4, a random value v'_4, and the previous upflow Fl'_3. Player U'_4 then sends downflow signal Fl'_4 to players U_1, U_2, and U'_3. When players U_1, U_2, and U'_3 receive the downflow signal Fl'_4, they may then use their private exponent values of χ to calculate the cryptographic key.

Table 4. Flows Associated With Two Players Joining An Initial Two Players

Fl_0	g			
Fl_1	g^{v_1}	$g^{v_1\chi_1}$		
Fl_2 Initial	$g^{v_1v_2\chi_2}$	$g^{v_1v_2\chi_1}$		
Fl'_2 Adjusted	$g^{v_1v'_2\chi'_2}$	$g^{v_1v'_2\chi_1}$	$g^{v_1v'_2\chi_1\chi'_2}$	
Fl'_3	$g^{v_1v'_2v'_3\chi'_2\chi'_3}$	$g^{v_1v'_2v'_3\chi_1\chi'_3}$	$g^{v_1v'_2v'_3\chi_1\chi'_2}$	$g^{v_1v'_2v'_3\chi_1\chi'_2\chi'_3}$

$F1'_4$	$g^{v_1v_2v_3v_4z_1z_2z_3z_4}$	$g^{v_1v_2v_3v_4z_1z_2z_4}$	$g^{v_1v_2v_3v_4z_1z_2z_4}$	$g^{v_1v_2v_3v_4z_1z_2z_3}$
Term →	β_1	β_2	β_3	β_4

Dynamic Secure Groups

[0067] It may be readily understood that groups may arbitrarily grow and shrink by sequential join and delete operations. Additionally, the join and delete operations may be simultaneously applied. This fluid nature of group size, with players coming and going, is why the term "dynamic" is used to describe such groups.

Distinct Secure Groups With Common Players

[0068] Refer now to Figure 3, where players U_1 ... U_4 form secure group 100. Another secure group 330 comprises players U_1 also in group 100, as well as U_A ... U_D. Additionally, another secure group 360 comprises players U_4 also in group 100, as well as U_X ... U_Z. Since player U_1 is a member of both groups 100 and 330, and since player U_4 is a member of both groups 100 and 360, it is possible for all players U_A ... U_D, U_1 ... U_4 and U_X ... U_Z to all intercommunicate. Players U_1 and U_4 would be required to translate from one secure group cryptographic key to the other, or in a sense act as a secure transmission router. In this manner, different secure groups may be joined by common players. Although not illustrated in Figure 3, a player may be in an unlimited number of groups, and group interconnection topologies are not limited.

Merging Of Distinct Secure Groups With Common Players

[0069] Although not described in Figure 3, some or all of the players U_1 ... U_4, U_A ... U_D and U_X ... U_Z may be merged into either a separate or distinct union of the secure dynamic groups. These operations would be straightforward applications of the setup and/or join operations previously described above.

[0070] Alternatively, it is possible for some or all players U_A ... U_D and U_X ... U_Z to be joined to initial group 100 formed initially by players U_1 ... U_4, thereby all players may intercommunicate directly by merging into one supergroup comprising players U_A ... U_D, U_1 ... U_4 and U_X ... U_Z. This may be accomplished by straightforward application of the join operation described above. Alternatively, by

taking advantage of already formed groups 330 and 360, a combination of join and refresh operations on the groups 330 and 360 may more rapidly be used to form a supergroup comprised of $U_A \ldots U_D$, $U_1 \ldots U_4$ and $U_X \ldots U_Z$.

Conclusion

[0071] All publications, patents, and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication or patent application were each specifically and individually indicated to be incorporated by reference.

[0072] The description given here, and best modes of operation of the invention, are not intended to limit the scope of the invention. Many modifications, alternative constructions, and equivalents may be employed without departing from the scope and spirit of the invention.

[0073] Arithmetic is in a finite cyclic group G=<alpha> of prime order beta. This group is assumed to be given a generator <alpha>. We assume that G, alpha, and beta are well-known. The group G should be a group on which the computational Diffie-Hellman problem is hard. There are three possibilities for such group: G = Z*p where p is a large prime number; G is an appropriate subgroup of Z*p; and G is an appropriate elliptic curve group.

[0074] Encryption methods may be instantiated by either the AES symmetric cipher or the bit-wise Boolean XOR-ing of the password with a public key.

CLAIMS

We claim:

1. A method for generating a cryptographic key by a player in a dynamic group, the method comprising:
   a) receiving,
      i) by a player U_p in a dynamic group with a first player U_1 and a last player U_n, where $p>1$,
      ii) a previous upflow $\mathbf{Fl}_{p-1}$ from a previous player U_{p-1} in the dynamic group;
   b) player U_p selecting a random value x_p , and a random value v_p ; and
   c) player U_p sending an outflow $\mathbf{Fl}_p$, comprising information based on the random value x_p , the random value v_p , and the previous upflow $\mathbf{Fl}_{p-1}$.
2. The method for generating a cryptographic key by a player in the dynamic group of claim 1, further comprising:
   a) for a first player U_1 in the dynamic group:
      i) player U_p selecting a random value x_1 , and a random value v_1 ;
      ii) setting an initial upflow $\mathbf{Fl}_1$ comprising information based on the random value x_1, the random value v_1 , and "g", a generator of a finite group where a computational solution to a Diffie-Hellman problem is hard.
3. The method for generating a cryptographic key by a player in the dynamic group of claim 2, the sending step further comprising:
   a) when player U_p is not the last player in the dynamic group, then:
      i) player U_p sending an upflow $\mathbf{Fl}_p$ to a subsequent player U_{p+1} in the dynamic group,
         (1) the upflow $\mathbf{Fl}_p$ comprising the outflow $\mathbf{Fl}_p$;
   b) when player U_p is the last player in the dynamic group, then:
      i) player U_p sending a downflow $\mathbf{Fl}_n$ to all other players in the dynamic group,
         (1) the downflow $\mathbf{Fl}_n$ comprising the outflow $\mathbf{Fl}_p$.
4. The method for generating a cryptographic key by a player in the dynamic group of claim 3 comprising:
   a) forming a set of L players, U_L , leaving the dynamic group;

b) forming a set of R players, U_R, remaining in the dynamic group;

c) choosing a controller U_C from the remaining set of R players U_R;

d) inputting, by controller U_C, the downflow $\mathbf{Fl}_n$,

i) where the downflow $\mathbf{Fl}_n$ has one entry associated with each player in the dynamic group; and

e) sending a controller U_C downflow signal $\mathbf{Fl}'_C$, comprising:

i) controller U_C sending the controller downflow $\mathbf{Fl}'_C$ based upon a random value x_C, a random value v_C, and the downflow signal $\mathbf{Fl}_n$,

(1) where each entry associated with the set of L players U_L leaving in the downflow signal $\mathbf{Fl}_n$ has been deleted.

5. The method for generating a cryptographic key by a player in the dynamic group of claim 3 comprising:

a) forming a set of J players to form a larger dynamic group $U_1, \ldots U_n, U_{n+1}, \ldots, U_{n+k}, \ldots, U_{n+J}$, where $1 \leq k \leq J$;

b) sending an upflow $\mathbf{Fl}_{n+k}$ from each player U_{n+k}, to player U_{n+k+1}, where $1 \leq k < J-1$,

i) said upflow $\mathbf{Fl}_{n+k}$ based upon a random value x_{n+k}, a random value v_{n+k}, and the upflow $\mathbf{Fl}_{n+k-1}$ received from player U_{n+k-1}; and

c) sending a downflow $\mathbf{Fl}_{n+J}$ by player U_{n+J}, based upon a random value x_{n+J}, a random value v_{n+J}, and the upflow $\mathbf{Fl}_{n+J-1}$.

6. The method for generating a cryptographic key by a player in the dynamic group of claim 3 comprising:

a) choosing a refresher U_r from the dynamic group $U_1, \ldots U_n$;

b) inputting, by refresher U_r, the downflow $\mathbf{Fl}_n$,

i) where the downflow $\mathbf{Fl}_n$ has one entry associated with each player in the dynamic group; and

c) sending, by refresher U_r, a refresher U_r downflow $\mathbf{Fl}'_r$ based upon a random value x_r, a random value v_r, and the downflow signal $\mathbf{Fl}_n$.

7. The method for generating a cryptographic key of claim 1 wherein said upflows are encrypted with a first encryption method.

8. The method for generating a cryptographic key of claim 3 wherein said downflows are encrypted with a second encryption method.
9. The method for generating a cryptographic key of claim 3 wherein said upflows and downflows are encrypted with a single encryption method.
10. An apparatus for generating a cryptographic key of claim 1.
11. The method for generating a cryptographic key of claim 1, wherein said steps are recorded on a computer readable medium.
12. The method for generating a cryptographic key of claim 1, wherein said upflows form a data structure transmitting through a computer readable medium.
13. The method for generating a cryptographic key of claim 1, wherein said steps are performed in a computer.
14. The method for generating a cryptographic key of claim 1, wherein said upflows are signal transmissions.
15. The method for generating a cryptographic key of claim 3, wherein said downflows are signal transmissions.
16. An apparatus for connecting a player to a dynamic group, the apparatus comprising a computer generating the cryptographic key of claim 1.
17. The method for generating a cryptographic key of claim 2 wherein said finite group is a finite cyclic group.
18. The method for generating a cryptographic key of claim 1, further comprising the step of:
    a) limiting the dynamic group to a size of three or more parties.

19. A method for generating a cryptographic key by a player in a dynamic group, the method comprising:
    a) providing a candidate player U_p wishing to be a party for a dynamic group with a first player U_1 and a last player U_n, where $p>1$,
    b) means for connecting player U_p to the dynamic group.
20. The method for generating a cryptographic key by a player in a dynamic group of claim 19, the method further comprising:
    a) means for removing a set of L players, U_L , leaving the dynamic group.

21. The method for generating a cryptographic key by a player in a dynamic group of claim 19, the method further comprising:

a) means for generating a downflow by the last player U_n in the dynamic group to the other players in the dynamic group.

22. The method for generating a cryptographic key by a player in a dynamic group of claim 19, the method further comprising:

a) means for joining a set of J player to the dynamic group.

FIG. 1A

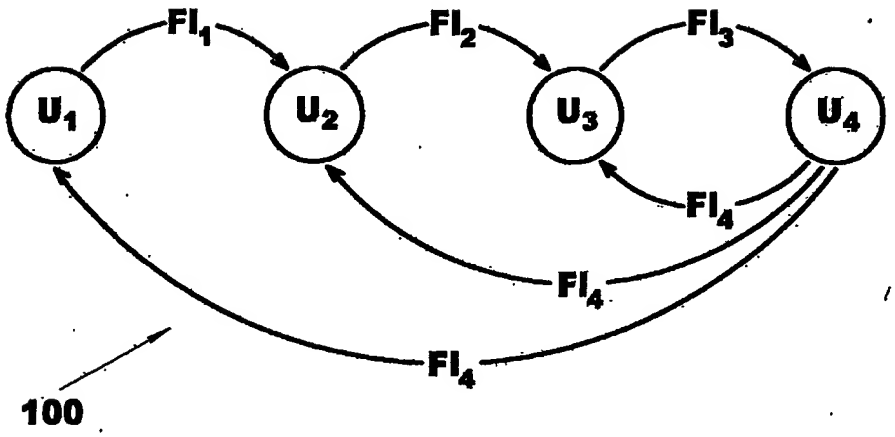


FIG. 1B

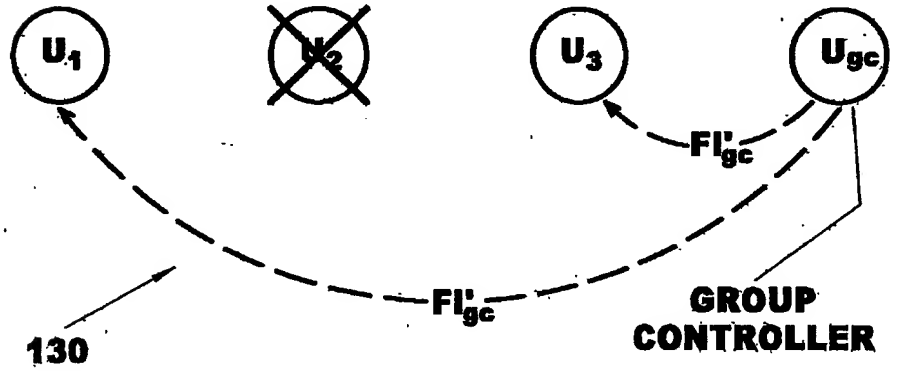


FIG. 1C

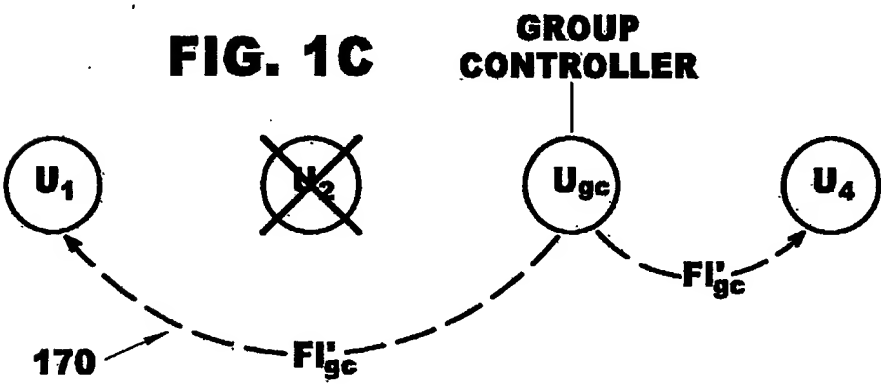


FIG. 2A

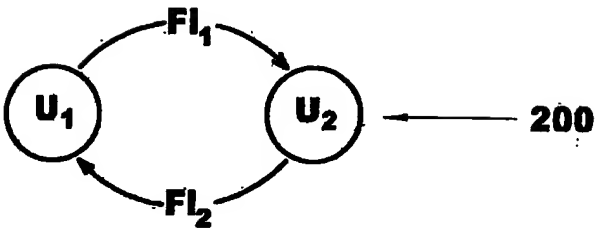


FIG. 2B

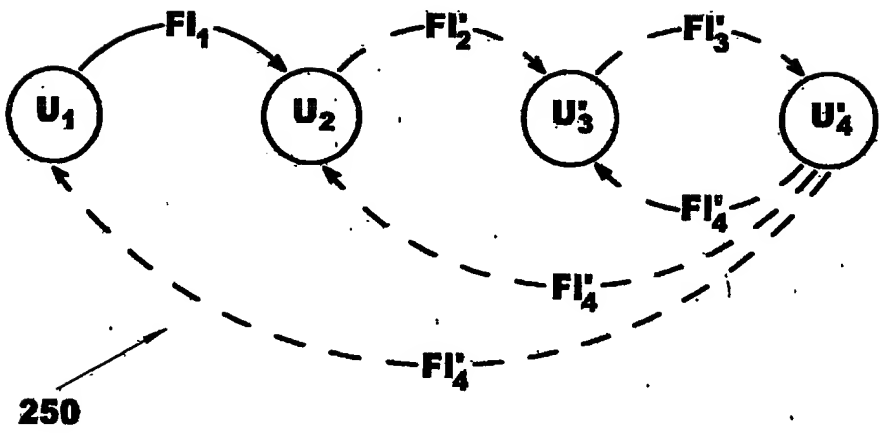


FIG. 3